网络安全技术

网络空间健康发展的保障

陈晓桦　武传坤◎主编

王海龙　徐克付◎副主编

中国工信出版集团　人民邮电出版社
POSTS & TELECOM PRESS

网络安全技术

网络空间健康发展的保障

陈晓桦　武传坤◎主编
王海龙　徐克付◎副主编

藏書 图书馆

人民邮电出版社
北京

图书在版编目（CIP）数据

网络安全技术 ：网络空间健康发展的保障 / 陈晓桦，武传坤主编. -- 北京 ：人民邮电出版社，2017.11
（网络强国系列丛书）
ISBN 978-7-115-45137-8

Ⅰ. ①网… Ⅱ. ①陈… ②武… Ⅲ. ①计算机网络－网络安全－研究－中国 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2017)第066466号

内 容 提 要

本书系统介绍网络安全的基本理论和关键技术，共 14 章。其中，第 1~7 章是基础技术，介绍网络安全概述、密码技术、身份认证、访问控制、网络攻击等；第 8~13 章是中级防护，介绍系统安全、反恶意代码、网络边界安全、网络服务安全、网络信息内容安全等 ；第 14 章是高级进阶，介绍云计算、大数据、物联网、工控网等网络安全。

本书旨在为全国各级领导干部提供网络安全方面的理论指南、实践指导和趋势指引，也可以作为从事网络安全技术研究、实践和管理等各类专业人士的培训教材。

◆ 主　　编　陈晓桦　武传坤
副 主 编　王海龙　徐克付
责任编辑　邢建春
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京隆昌伟业印刷有限公司印刷

◆ 开本：720×960　1/16
印张：17.5　　2017 年 11 月第 1 版
字数：210 千字　　2017 年 11 月北京第 1 次印刷

定价 108.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

序 言

网络强国是国家强盛和民族振兴的重要内涵和体现，是实现中华民族伟大复兴中国梦的关键一环和必由之路。实施网络强国战略，这是党中央顺应时代要求和发展潮流，站在推动国家创新发展、促进经济转型升级、实现成果普惠民众、打造网络治理体系、保障国家信息安全的战略高度，就我国互联网未来发展的目标愿景和建设要求，精心描绘的宏伟战略。

为了实现这一宏伟战略目标，2014 年 2 月，习近平总书记在中央网络安全和信息化领导小组第一次会议上明确指出："网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国""建设网络强国，要把人才资源汇聚起来，建设一支政治强、业务精、作风好的强大队伍"。

2016 年 4 月，习近平总书记在网络安全和信息化工作座谈会上明确指出"各级党政机关和领导干部要学会通过网络走群众路线，经常上网看看，了解群众所思所愿，收集好想法好建议，积极回应网民关切、解疑释惑""新形势下，善于运用网络了解民意、开展工作，是领导干部做好工作的基本功，是衡量领导干部治理能力和水平的重要方面，各级干部特别是领导干部务必不断提高这项本领"。2016

年 10 月， 习近平总书记在主持中央政治局就实施网络强国战略进行第三十六次集体学习时强调： “各级领导干部特别是高级干部， 如果不懂互联网、 不善于运用互联网， 就无法有效开展工作。 各级领导干部要学网、 懂网、 用网， 积极谋划、 推动、 引导互联网发展。 要正确处理安全和发展、 开放和自主、 管理和服务的关系， 不断提高对互联网规律的把握能力、 对网络舆论的引导能力、 对信息化发展的驾驭能力、 对网络安全的保障能力， 把网络强国建设不断推向前进”。

2016 年 11 月， 《中华人民共和国网络安全法》 正式颁发， 再次凸显出网络安全已经成为关系国家安全和发展、 关系广大人民群众切身利益的重大问题。 在此背景下， 作为参与网络强国战略决策和实施的领导干部， 必须具备网络和网络安全的知识与技能。 因此， 需要一系列高屋建瓴、 通俗易懂的与网络安全密切相关的学习读本。 根据上述要求， 我们开展了网络安全领域的调研工作， 并组织专家编写本书。

自 2015 年起， 中国网络空间安全协会以自愿申领与定向邀请相结合的方式组织编写了一系列网络安全培训教材。 为提高本书的针对性和易读性， 我们组织业内专家对上述网络安全教材进行了知识点调整、内容缩减、 语言梳理， 完成了此次编写和统稿工作。

衷心希望本书能够提高各级领导干部的网络安全知识与技能， 为加快推进高素质网络人才队伍培养和网络强国建设做出应有的贡献。

中国工程院院士 方滨兴

2016 年 12 月 6 日

此为试读，需要完整PDF请访问：www.ertongbook.com

前 言

当前， 网络空间已经成为继陆、 海、 空、 天之后的第五疆域，覆盖政治、 经济、 文化、 社会、 军事、 外交等各个领域并深入到社会生活的各个层面。 网络空间安全在经济和社会发展的关键环节和基础保障方面日趋重要， 已成为国家安全的核心组成部分， 更为 “实施网络强国战略” 起着保驾护航的无可替代作用。

随着人、 机、 物三元融合发展趋势在信息技术领域的不断演进，网络空间的安全形势日益严峻， 各种各样的网络安全隐患急剧增多，渗透和反渗透、 破坏和反破坏、 黑客和反黑客的斗争愈演愈烈， 不仅影响了网络的稳定运行和用户的正常使用， 造成重大经济损失， 而且还严重威胁到国家安全。 为了构建完备的网络安全管理与攻防体系，需要在完善网络安全法规标准的基础上， 积极探索、 努力发展更加有效的网络安全手段。 因此， 网络安全的意识提高、 基本运用、 体系建设、 创新驱动等显得越来越重要， 并受到各个国家的高度重视。

作为网络强国战略学习读本， 本书系统介绍了网络安全的基本理论和关键技术， 共 14 章。 第 1~7 章是基础技术， 包括网络安全概述、互联网协议安全、 密码技术、 身份认证、 访问控制、 网络攻击以及物理与人员安全等； 第 8~13 章是中级防护， 包括系统安全、 反恶意

代码、网络边界安全、网络服务安全、移动网络安全以及网络信息内容安全等；第 14 章是高级进阶，包括云计算、大数据、物联网、工控网等新技术与新应用面临的网络安全挑战。

方滨兴院士对本书的编写组织工作给予了悉心指导，陈晓桦研究员和武传坤研究员负责本书的整体筹划和内容安排以及统稿，王海龙工程师和徐克付副研究员负责本书的组稿审核。同时，对各位参与编写工作的专家学者表示感谢！

由于时间仓促，编者学识水平有限，谬误之处难免，恳请读者批评指正！

目 录

第 1 章 网络安全概述 // 001
1.1 网络安全现状 // 002
1.1.1 网络安全现状及影响 // 003
1.1.2 网络安全问题的来源 // 004
1.2 网络安全挑战 // 005
1.2.1 传统的网络威胁 // 005
1.2.2 网络安全的新挑战 // 006
1.3 网络安全体系 // 007
1.3.1 网络安全防护体系 // 007
1.3.2 网络安全信任体系 // 009
1.3.3 网络安全保障体系 // 011
1.4 网络安全标准法规 // 013
1.4.1 网络安全标准 // 014
1.4.2 网络安全法律法规 // 017

第 2 章 互联网协议安全 // 019
2.1 引言 // 020
2.2 TCP/IP 栈 // 021
2.2.1 TCP/IP 栈简介 // 022
2.2.2 OSI 网络分层参考模型 // 023
2.2.3 TCP/IP 参考模型 // 024
2.3 TCP/IP 安全性分析 // 026
2.3.1 TCP/IP 攻击的分类 // 027
2.3.2 TCP/IP 攻击利用的常见协议漏洞 // 028
2.4 网络安全协议 // 031
2.5 网络安全协议的安全问题 // 033

第 3 章　密码技术 // 035
3.1　密码学概述 // 036
3.1.1　起源与发展 // 037
3.1.2　加密体制简介 // 038
3.1.3　加密体制的分类 // 039
3.1.4　现代密码学中的其他重要分支 // 040
3.2　数据加密技术 // 041
3.2.1　私钥加密体制——流密码 // 041
3.2.2　对称密钥加密体制——分组密码 // 043
3.2.3　公开密钥加密体制 // 047
3.4　国家标准密码算法简介 // 048

第 4 章　身份认证 // 053
4.1　身份认证概述 // 054
4.2　身份认证机制 // 055
4.3　对“人”的认证 // 056
4.3.1　基于口令的认证 // 057
4.3.2　双因子身份认证技术 // 059
4.3.3　生物特征识别认证技术 // 059
4.4　对“机”的认证 // 060
4.5　对“物”的认证 // 061
4.6　其他身份认证技术 // 061

第 5 章　访问控制 // 063
5.1　访问控制模型与管理 // 064
5.1.1　访问控制基本概念 // 064
5.1.2　访问矩阵 // 067
5.1.3　自主访问控制 // 068
5.1.4　强制访问控制 // 069
5.1.5　基于角色的访问控制 // 070
5.1.6　基于任务的访问控制模型 // 071
5.2　访问控制安全策略简介 // 071
5.3　访问控制实现技术 // 073
5.3.1　访问控制列表与能力列表 // 073

5.3.2 访问控制决策中间件 // 074
5.3.3 信任管理技术 // 076

第 6 章 网络攻击技术 // 079
6.1 网络攻击概述 // 080
6.1.1 网络攻击的定义 // 080
6.1.2 网络攻击原因解析 // 081
6.2 网络攻击的常用技术方法 // 082
6.2.1 端口扫描 // 082
6.2.2 口令破解 // 083
6.2.3 缓冲区溢出 // 084
6.2.4 拒绝服务攻击 // 085
6.2.5 信息窃密 // 090
6.3 高级持续性威胁 // 091
6.3.1 高级持续性威胁概述 // 091
6.3.2 APT 与传统恶意代码攻击的对比 // 093
6.3.3 APT 攻击手段 // 094
6.3.4 APT 检测和防御 // 096

第 7 章 物理与人员安全 // 099
7.1 物理安全 // 100
7.1.1 物理安全概述 // 100
7.1.2 机房环境安全 // 101
7.1.3 电磁安全 // 104
7.1.4 物理隔离 // 104
7.1.5 物理设备安全 // 105
7.2 人员安全 // 106
7.2.1 人员安全管理概述 // 106
7.2.2 教育与培训 // 107
7.2.3 安全审查管理 // 110

第 8 章 系统安全 // 113
8.1 操作系统安全 // 114
8.1.1 操作系统安全概述 // 114
8.1.2 操作系统面临的安全问题 // 117

8.1.3 操作系统的安全机制 // 118
8.2 可信计算 // 121
8.2.1 可信计算概述 // 121
8.2.2 可信计算技术 // 123
8.3 数据库安全 // 125
8.3.1 数据库安全概述 // 125
8.3.2 数据库安全技术 // 128
8.3.3 数据库安全防护策略 // 130
8.4 个人数据安全 // 131
8.4.1 个人数据安全概述 // 131
8.4.2 个人数据安全面临的问题 // 132
8.4.3 个人数据安全保护技术 // 132
8.5 备份与恢复 // 133
8.5.1 备份与恢复 // 133
8.5.2 灾难备份 // 134

第 9 章 反恶意代码 // 135
9.1 分类与特征 // 137
9.2 结构与原理 // 139
9.3 反病毒引擎 // 140
9.4 清除防范技术 // 141
9.5 不同平台下的恶意代码查杀 // 144

第 10 章 网络边界安全 // 159
10.1 防火墙技术 // 160
10.2 入侵检测与防御 // 162
10.2.1 为什么需要入侵检测系统 // 163
10.2.2 入侵检测系统的基本组成 // 163
10.2.3 入侵检测系统的常规分类 // 164
10.2.4 入侵检测的技术手段 // 165
10.2.5 入侵检测的前景 // 167
10.2.6 入侵防御系统 // 168
10.3 虚拟专用网络 // 169

此为试读，需要完整PDF请访问：www.ertongbook.com

第 11 章　网络服务安全 // 177

11.1　Web 安全 // 178
11.1.1　Web 与脚本程序安全概述 // 179
11.1.2　Web 安全增强手段 // 181
11.1.3　Web 欺骗技术 // 181
11.1.4　电子交易安全 // 183
11.2　域名服务安全 // 184
11.3　电子邮件安全 // 186
11.3.1　电子邮件安全概述 // 186
11.3.2　电子邮件欺骗技术与典型实例 // 189
11.3.3　配置 Microsoft Outlook // 191
11.4　网络文件服务安全 // 193
11.5　其他常用互联网典型应用服务安全 // 194
11.5.1　搜索引擎服务安全 // 194
11.5.2　即时通信工具安全 // 197

第 12 章　无线网络安全 // 199

12.1　移动网络安全 // 200
12.1.1　无线广域网安全要求概述 // 201
12.1.2　2G 安全机制 // 202
12.1.3　3G 安全机制 // 204
12.1.4　4G 安全机制 // 207
12.1.5　5G 安全机制 // 213
12.2　无线局域网安全 // 214
12.2.1　无线局域网 // 214
12.2.2　无线局域网面临的安全问题 // 215
12.2.3　无线局域网安全性 // 217
12.3　近距离无线通信网络安全 // 218
12.3.1　射频识别安全 // 219
12.3.2　近场通信安全 // 220
12.3.3　无线传感器网络安全 // 221

第 13 章　网络信息内容安全 // 223
13.1　网络信息内容安全技术 // 224

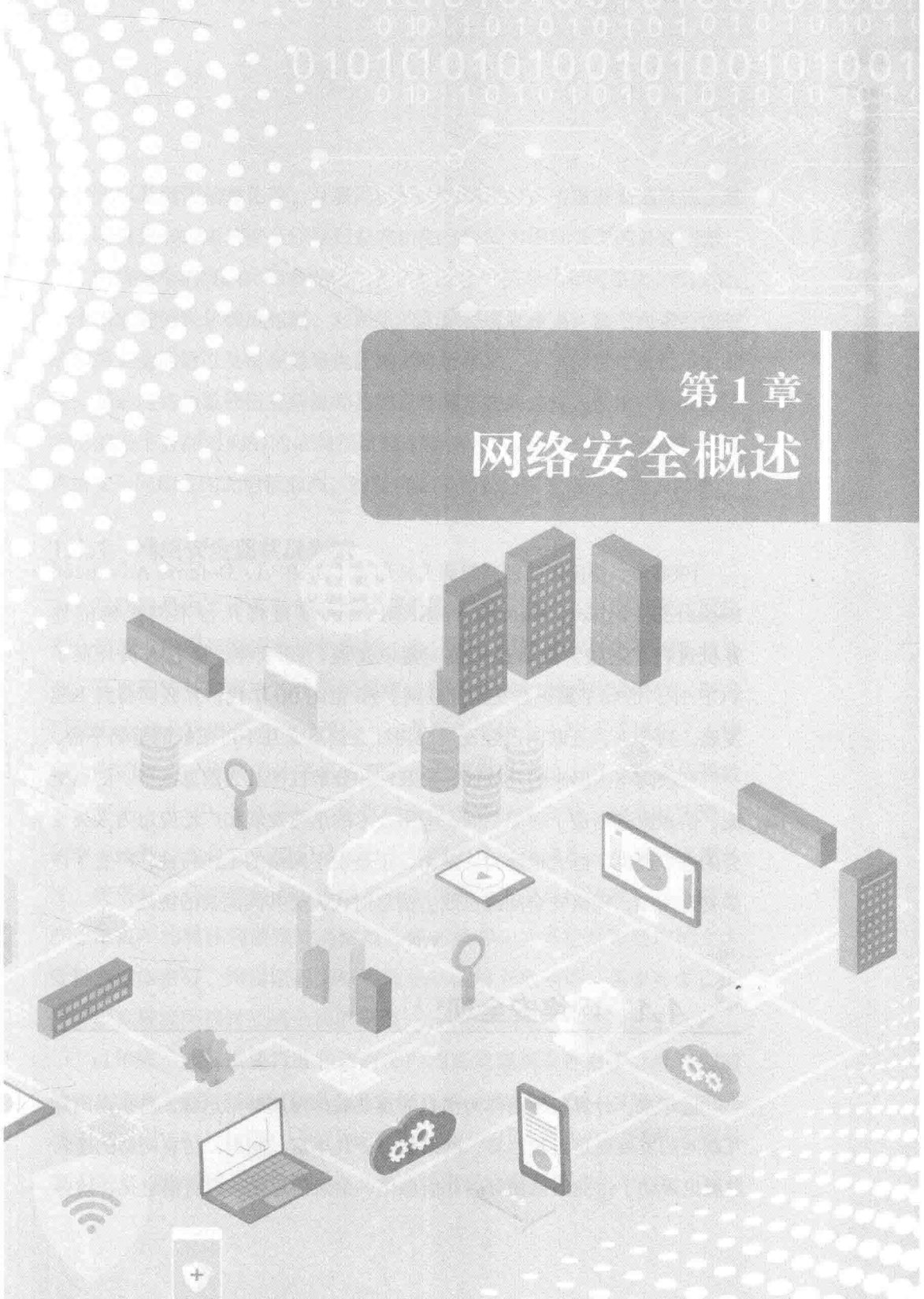
13.1.1 网络内容安全技术概述 // 224
13.1.2 信息内容采集、过滤、审计技术 // 225
13.2 网络舆情分析 // 229
13.2.1 网络舆情定义 // 229
13.2.2 网络舆情分析概述 // 229
13.2.3 网络舆情分析关键技术 // 230
13.2.4 话题跟踪与热点识别 // 234
13.3 社交网络安全 // 235
13.3.1 社交网络安全现状 // 235
13.3.2 社交网络的安全隐患 // 235
13.3.3 社交网络安全的技术解决方案 // 236
13.3.4 提供社交网络安全的管理措施 // 238

第 14 章 新技术与新应用的网络安全 // 241

14.1 云安全 // 242
14.1.1 云安全概述 // 242
14.1.2 云安全面临的挑战 // 243
14.1.3 云安全技术的主要内容 // 245
14.1.4 云安全服务体系 // 246
14.2 大数据安全 // 247
14.2.1 大数据安全概述 // 247
14.2.2 大数据安全面临的问题及挑战 // 248
14.2.3 大数据安全技术现状 // 251
14.3 物联网安全 // 255
14.3.1 物联网安全概述 // 255
14.3.2 物联网安全面临的挑战 // 258
14.3.3 物联网安全特征 // 259
14.3.4 物联网安全技术现状 // 260
14.4 工控网络安全 // 262
14.4.1 工控网络安全概述 // 262
14.4.2 工控网络安全面临的挑战 // 263
14.4.3 工控网络安全的特征 // 264
14.4.4 工控网络安全技术现状 // 265

参考文献 // 267

第1章
网络安全概述



1969年，美国国防部高级研究计划局（DARPA，Defense Advanced Research Projects Agency）的ARPAnet项目将几台不同机构的计算机进行了连接，随后这一技术得以发展，1979年，研究人员开发了TCP/IP，形成了真正意义的互联网。20世纪90年代，互联网得到飞速发展。到今天，互联网已经发展成为社会信息交互不可或缺的基础平台。

互联网与生俱来的开放性、交互性和分散性使其为信息共享、信息交流、信息服务创造了理想空间，网络技术的迅速发展和广泛应用为人类社会的进步提供了巨大推动力。然而，正是由于网络的上述特性，产生了许多安全问题，网络安全问题已成为信息时代人类共同面临的挑战。

1.1 网络安全现状

近年来，计算机网络作为信息的重要载体发展非常迅猛，特别是国际互联网的发展更是日新月异，网络服务极其丰富。同时，信息网络的蓬勃发展也带动了企业信息化、商业信息化、金融信息化、教育信息化、政务

信息化以及国防信息化等，互联网已经成为国民经济的重要基础设施，然而，网络发展带来的安全问题日益突出，已经成为困扰各国的共性问题。

网络安全的复杂化和多元化主要在于社会的信息化和网络化，可以说，一个国家的信息化程度越高，对网络的依赖程度就越高，随之而来所面临的网络安全问题以及潜在隐患也就越多。近年来，中国信息化进程不断加快，基础网络与重要信息系统等基础设施基本建成并投入使用，社会经济生活的各个方面对网络的依赖程度越来越高，大有牵一发而动全身之势，网络安全问题也因此愈演愈烈，给经济增长和社会稳定带来了巨大隐患。

1.1.1 网络安全现状及影响

互联网是为了计算机的互联互通而设计的，设计之初没有考虑网络安全问题。随着互联网规模的膨胀，网络安全问题逐步显现并越来越复杂。各种网络基础应用、计算机系统、Web 程序的漏洞层出不穷，普通网民安全意识及相关知识的匮乏，这些都为网络上不法分子提供了入侵和偷窃的机会。最初的计算机病毒制造者通常以炫技、恶作剧或仇视破坏为目的。从 2000 年开始，病毒制造者逐渐变得贪婪，越来越多地以获取经济利益为目的。他们通过分工明确的产业化操作，从病毒程序开发、传播病毒到销售病毒，形成了分工明确的整条操作流程，这条黑色产业链每年的整体利润预计高达数亿元。黑客和计算机病毒窃取的个人资料从 QQ 密码、网游密码到银行账号、信用卡账号等，包罗万象，任何可以直接或间接转换成金钱的东西，都成为不法分子窃取的对象。

近年来，涉及重要行业和政府部门的高危漏洞事件增多。针对漏洞的挖掘和利用研究日趋活跃。国家信息安全漏洞库（CNNVD，China National Vulnerability Database of Information Security）新增收录漏洞数量年均增长率在 15% ~ 25%，其中高危漏洞约占$\frac{1}{4}$。

可见，网络安全不仅影响普通网民信息和数据的安全性，而且全面渗透到国家政治、经济、军事、社会稳定等各个领域，严重影响一个国家的健康发展。

1.1.2 网络安全问题的来源

互联网最初是在几个科研教育服务计算机中心互连的基础上建立起来的，其总体架构和其所使用的 TCP/IP 的设计均是在基于可信环境的前提下完成，因此互联网设计之初并未考虑网络安全问题。

互联网的安全性问题不仅源于其开放性，而且 TCP/IP 族的设计也缺乏安全性考虑。在网络层，由于 IP 缺乏安全认证和保密机制，因此容易受到各种攻击；在传输层，虽然 TCP 在建立连接时有“三次握手”，但只是简单的应答，其连接能被欺骗、截取及操纵，而 UDP 易受到 IP 源路由和拒绝服务的攻击；在应用层，传统的服务 HTTP、FTP、Telnet、SMTP、POP3、DNS、SNMP 等均缺乏较高的可认证性、完整性和保密性，因此，几乎没有安全性可言。

网络应用更成为黑客及病毒的攻击重点。网络应用丰富，可供病毒传播利用的途径越来越复杂。例如，随着网络视频和音乐的发展，U 盘、MP3 等可移动介质广泛被黑客利用来传播病毒；厂商在保护用户利益上投入的精力远远不够，使即时通信软件和网络游戏都是重要的病毒传播渠道和被害对象；网络银行和网络证券交易日益火爆，针对网络银行和证券的木马、后门程序暴增，大量缺乏基本安全意识和防护措施的股民则面临着更大安全风险。

为了提供网络安全保护，在 IP 层，研究人员开发了 IPSec 协议。互联网工程工作小组（IETF，Internet Engineering Task Force）历经 3 年研究，于 1998 年形成了关于 IPv6 的第一个协议 RFC 2460。在

此为试读，需要完整PDF请访问：www.ertongbook.com